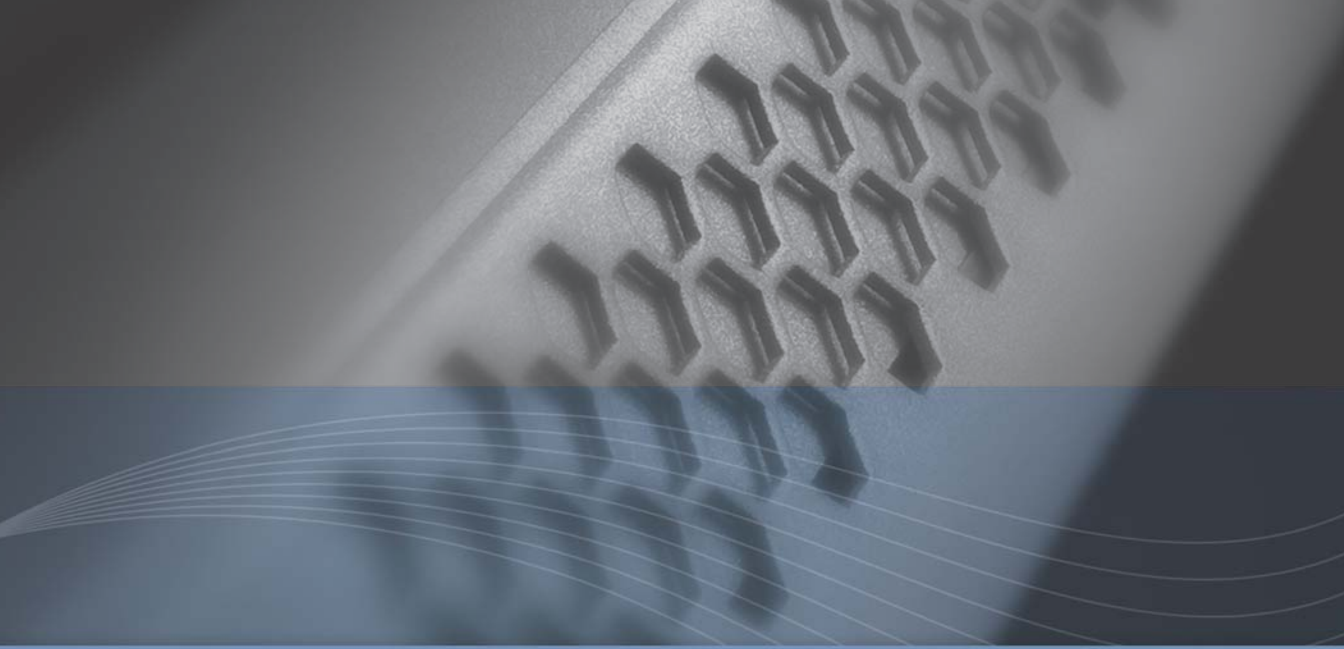


Global Management System (GMS) **7.0 Getting Started Guide**

SonicWALL® E-CLASS

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS™

SonicWALL GMS 7.0
Getting Started Guide

This *Getting Started Guide* contains installation procedures and configuration guidelines for deploying SonicWALL Global Management System (SonicWALL GMS) on a Windows server on your network. SonicWALL GMS is a Web-based application that can configure, manage, and monitor the status of thousands of SonicWALL Internet security appliances and non-SonicWALL appliances from a central location. SonicWALL GMS provides the following benefits:

- Centralized security and network management
- Sophisticated VPN deployment and configuration
- Active device monitoring and alerts
- Intelligent reporting and activity visualization
- Centralized logging and offline management

Note: *For complete documentation, refer to the **SonicWALL GMS Administrator's Guide**. This and other documentation are available at:* http://www.sonicwall.com/us/Support.html
For the latest SonicWALL GMS software version downloads and documentation, login to the MySonicWALL website at: http://www.mysonicwall.com.

Contents

This document contains the following sections:

1 "Before You Begin" on page 3

- "System Requirements" on page 3
- "Record Configuration Information" on page 7

2 "Installing and Upgrading SonicWALL GMS" on page 8

- "Installing Universal Management Suite 7.0" on page 8
- "Upgrading From an Earlier Version of SonicWALL GMS" on page 12

3 "Registering and Licensing SonicWALL GMS" on page 14

- "Registering / Licensing SonicWALL GMS After a Fresh Install" on page 14
- "Registering Associated Servers in a Distributed Deployment" on page 17

4 "Selecting the Role for a SonicWALL GMS Server" on page 18

- "Using the Role Configuration Tool" on page 19
- "Manually Configuring the System Role" on page 22

5 "Introduction to the Management Interfaces" on page 32

- "Overview of the Two Interfaces" on page 32
- "Switching Between Management Interfaces" on page 33
- "SonicWALL UMH System Interface Introduction" on page 33
- "SonicWALL GMS Management Interface Introduction" on page 34

6 "Next Steps" on page 40

1 Before You Begin

See the following sections for information about SonicWALL GMS:

- “System Requirements” on page 3
- “Record Configuration Information” on page 7

System Requirements

The SonicWALL GMS 7.0 software comes with a base license to manage either 10 nodes or 25 nodes. You can purchase additional licenses on MySonicWALL. For more information on licensing additional nodes, visit: http://www.sonicwall.com/us/Products_Solutions.html

Before installing SonicWALL GMS, review the following requirements.

Operating System Requirements

The SonicWALL GMS 7.0 release supports the following operating systems:

- Windows Server 2003 32-bit and 64-bit (SP2)
- Windows Server 2008 SBS R2 64-bit
- Windows Server 2008 R2 Standard 32 bit and 64 bit

Tip: *In all instances, SonicWALL GMS is running as a 32-bit application. Bundled databases run in 64-bit mode on 64-bit Windows operating systems. All listed operating systems are supported in both virtualized and non-virtualized (VMware ESXi 4.1) environments.*

Hardware for Windows Server

- x86 Environment: Minimum 3 GHz processor dual-core CPU Intel processor
- 4GB RAM
- 300 GB disk space

For Windows Server 64-bit, the higher the amount of RAM memory provides better performance for the SonicWALL GMS management, reporting, and monitoring modules.

Database Requirements

SonicWALL GMS 7.0 supports the following databases:

- Microsoft SQL Server 2000 (SP4)
- Microsoft SQL Server 2005 (SP1)
- Microsoft SQL Server 2008

Regarding MS SQL Server 2005, SonicWALL GMS supports:

- SQL Server 2005 Workgroup
- SQL Server 2005 Standard
- SQL Server 2005 Enterprise

Note: *SonicWALL GMS does* ***not*** *support MS SQL Server 2005 Express.*

- SonicWALL MySQL Install Package installed on either Windows 2000 Server (SP4) or 2003 Server (SP1)

MySQL Requirements

SonicWALL GMS automatically installs MySQL as part of the base installation package. Separately installed instances of MySQL is not supported with SonicWALL GMS 7.0. Separately installed instances of MySQL is supported with SonicWALL GMS 6.0 only.

Java Requirements

SonicWALL GMS services uses **Java SE 6 Update 23**. SonicWALL GMS automatically downloads the Java Plug-in 6.0 when accessing SonicWALL GMS. SonicWALL GMS uses **Tomcat 6.0.32**.

Browser Requirements

- Microsoft Internet Explorer 8.0 or higher
- Mozilla Firefox 7.0 or higher
- Google Chrome 14.0 or higher

Network Requirements

To complete the SonicWALL GMS deployment process documented in this *Getting Started Guide*, the following network requirements must be met:

- The SonicWALL GMS server must have access to the Internet
- The SonicWALL GMS server must have a static IP address
- The SonicWALL GMS server’s network connection must be able to accommodate at least 1 KB/s for each device under management. For example, if SonicWALL GMS is monitoring 100 SonicWALL appliances, the connection must support at least 100 KB/s.

Alert: *Depending on the configuration of SonicWALL log settings and the amount of traffic handled by each device, the network traffic can vary dramatically. The 1 KB/s for each device is a general recommendation. Your installation requirements may vary.*

SonicWALL Appliance and Firmware Support

SonicWALL Platforms	SonicWALL Firmware Version
Firewall / VPN	
SuperMassive 10000 Series	SonicOS 6.0 or newer
NSA Series	SonicOS 5.0 or newer
TZ Series	SonicOS Enhanced 3.2 or newer SonicOS Standard 3.1 or newer
PRO Series	SonicOS Enhanced 3.2 or newer
SonicWALL CSM Series	SonicOS CF 2.0 or newer
Secure Remote Access	
SonicWALL SMB SRA Series	SonicOS SSL-VPN 2.0 or newer (management) SonicOS SSL-VPN 2.1 or newer (reporting)
SonicWALL Aventail EX-Series	Aventail 9.0 or newer
Backup and Recovery	
SonicWALL CDP Series	SonicWALL CDP 2.3 or newer (management) SonicWALL CDP 5.1 or newer (reporting)
Email Security / Anti-Spam	
SonicWALL Email Security Series	SonicWALL Email Security 7.2 or newer (management only)

Note: *Legacy SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2, and SonicWALL Pro/Pro-VX models are not supported for SonicWALL GMS management. Appliances running SonicWALL legacy firmware including SonicOS Standard 1.x and SonicWALL legacy firmware 6.x.x.x are not supported for SonicWALL GMS management.*

Non-SonicWALL Appliance Support

SonicWALL GMS provides monitoring support for non-SonicWALL TCP/IP and SNMP-enabled devices and applications.

SonicWALL GMS Gateway Recommendations

A GMS gateway is a SonicWALL firewall appliance that allows for secure communication between the SonicWALL GMS server and the managed appliance(s), using VPN tunnels.

A GMS gateway is not required in all deployment scenarios, but when deployed, the GMS gateway must be a SonicWALL VPN-based network security appliance running SonicOS Enhanced firmware or another VPN device that is interoperable with SonicWALL VPN. The GMS gateway provides a VPN management tunnel for each managed appliance. The number of management tunnels depends on the number of VPNs supported by the GMS gateway appliance and may be a limiting factor.

For complete information about SonicWALL GMS management methods and requirements for a GMS Gateway, see the **GMS Gateway Requirements** section in the *SonicWALL GMS Administrator's Guide*, available on: http://www.sonicwall.com/us/Support.html

Record Configuration Information

Before continuing, record the following configuration information for your reference.

SonicWALL GMS Information

SMTP Server Address: ________________	The IP address or host name of your Simple Mail Transfer Protocol (SMTP) server. For example, mail.emailprovider.com.
HTTP Web Server Port: ________________	The number of your Web server port if customized. The default port is 80.
HTTPS Web Server Port: _______________	The number of your secure (SSL) Web server port if customized. The default port is 443.
GMS Administrator Email 1: ____________	The email address of a SonicWALL GMS administrator who will receive email notifications from SonicWALL GMS.
GMS Administrator Email 2: ____________	The email address of an additional SonicWALL GMS administrator who will receive email notifications from SonicWALL GMS. This field is optional.
Sender Email Address: ________________	The email address from which the email notifications will be sent by SonicWALL GMS.
GMS Gateway IP: _____________________	The IP address of the SonicWALL GMS gateway between the SonicWALL GMS agent and the network. This optional field is only applicable if you have a GMS gateway.
GMS Gateway Password: ______________	The password for the SonicWALL GMS gateway. This optional field is only applicable if you have gateway between the SonicWALL GMS and the network.
Database Vendor: _____________________	Your database vendor if you are using a SQL Server database.
Database Host/IP: _____________________	The IP address of the database host. This is not required when using the bundled database on this server.
Database User:________________________	The MySQL user name for the database administrator. This is not required when using the bundled database on this server. Refer to "Configuring Database Settings" on page 28.
Database Password:__________________	The MySQL password for the database administrator. This is not required when using the bundled database on this server.

2 Installing and Upgrading SonicWALL GMS

SonicWALL GMS can be configured for a single server or in a distributed environment on multiple servers.

SonicWALL GMS 7.0 can be installed as a fresh install or as an upgrade from GMS 6.0.

Note: *You must disable the User Account Control (UAC) feature on Windows before running the SonicWALL GMS installer. In addition, disable Windows Firewall or your personal firewall before running this installer.*

This section contains the following subsections:

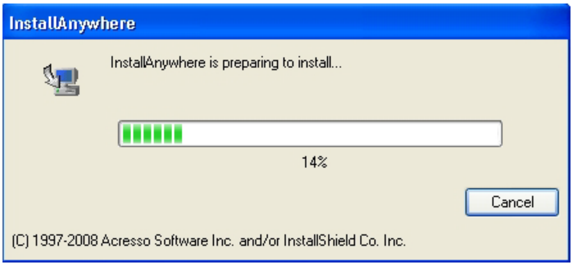
- "Installing Universal Management Suite 7.0" on page 8
- "Upgrading From an Earlier Version of SonicWALL GMS" on page 12

Installing Universal Management Suite 7.0

In SonicWALL GMS 7.0, all software components related to SonicWALL GMS and SonicWALL Analyzer, including the MySQL database, executable binary files for all GMS services, and other necessary files, are installed using the Universal Management Suite 7.0 single-binary installer. All GMS and Analyzer files are installed as the Universal Management Suite 7.0, but no distinction is made between GMS and Analyzer during the installation. The initial installation phase takes just a few minutes for any type of installation, such as GMS server, Analyzer server, database server, or any other role.

To perform a fresh install of the Universal Management Suite 7.0 from the single binary installer, perform the following steps:

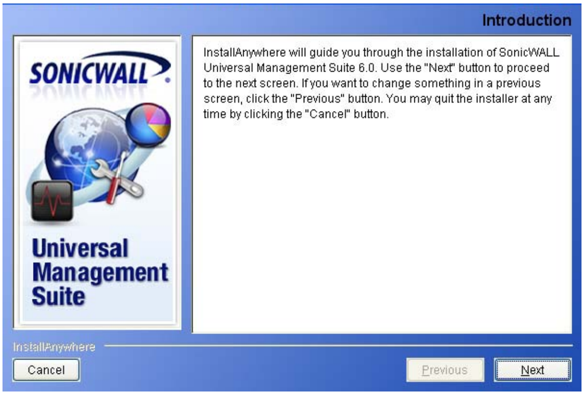
1. Log on to your SonicWALL GMS management computer as **administrator** (Windows). Launch the SonicWALL Universal Management Suite 7.0 installer, by right-clicking the file **sw_gmsvp_win_eng_7.0.xxxx.xxxx.exe** (where "xxxx" represent the exact version numbers) and select **Run as administrator**. It may take several seconds for the InstallAnywhere self-extractor to initialize.



InstallAnywhere is preparing to install...

(C) 1997-2008 Acresso Software Inc. and/or InstallShield Co. Inc.

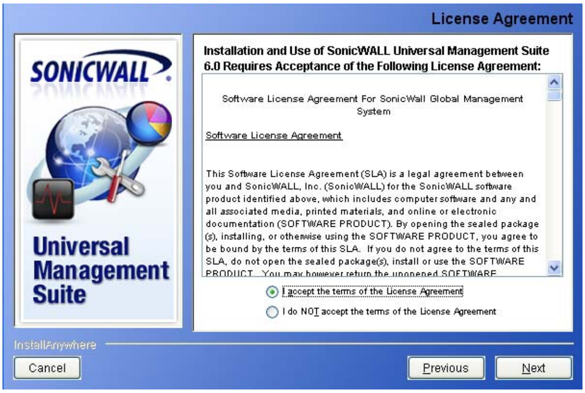
2. In the Introduction screen, click **Next.**



Introduction

InstallAnywhere will guide you through the installation of SonicWALL Universal Management Suite 6.0. Use the "Next" button to proceed to the next screen. If you want to change something in a previous screen, click the "Previous" button. You may quit the installer at any time by clicking the "Cancel" button.

3. In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next.**



License Agreement

Installation and Use of SonicWALL Universal Management Suite 6.0 Requires Acceptance of the Following License Agreement:

Software License Agreement For SonicWall Global Management System

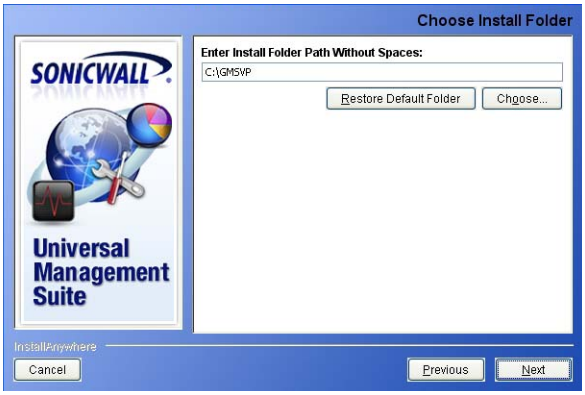
Software License Agreement

This Software License Agreement (SLA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package (s), installing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this SLA. If you do not agree to the terms of this SLA, do not open the sealed package(s), install or use the SOFTWARE PRODUCT. You may however return the unopened SOFTWARE

● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

4. Select the path to the folder where you would like to install the files. You can accept the default path, **C:\GMSVP**, type in a new path, or click the **Choose** button to navigate to the selected folder. When you are finished, click **Next**.



Choose Install Folder

Enter Install Folder Path Without Spaces:

C:\GMSVP

Alert: *Do not include spaces in the installation path.*

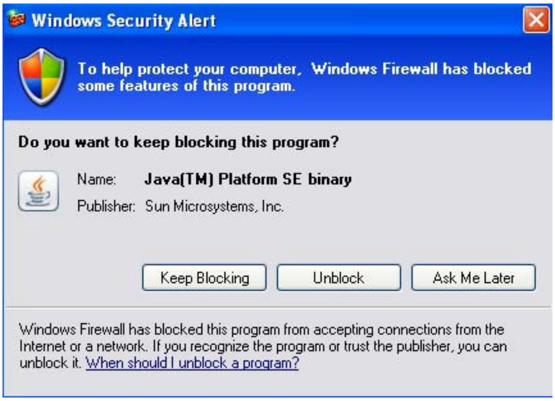
5. In the SonicWALL Universal Management Suite Settings screen, select or type in the IP address to which the SonicWALL GMS services should bind to listen for inbound TCP, UDP, SNMP, syslog, or other packets. The installer detects and offers radio buttons for any IP addresses associated with the system. The default is your management computer IP address. To use a different IP address, select **Other** and type the IP address into the field. Click **Next.**
6. To use a custom port for HTTP or HTTPS traffic to the system's Web Server, type the port number into the **HTTP Port** or **HTTPS Port** field.

   If you receive the message "Cannot bind to the port number specified. Please specify a different one," the port you specified is in use by another program, for example, Internet Information Services (IIS). Specify a different, unused port, such as 8080.

Tip: *If you specify a custom port, you will need to modify the URLs you use to access GMS by using the following format:* ***http://localhost:<port>/*** *(to login from the local host) or* ***http://<ipaddress>:<port>/*** *(to login from a remote location). For example, if you specified HTTP port 8080, the URL would be* ***http://localhost:8080/*** *for a local host login, or* ***http://10.0.93.20:8080/*** *for a remote login.*

7. Click **Install.**

8. If you see a Windows Security Alert for Java, click **Unblock**.



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

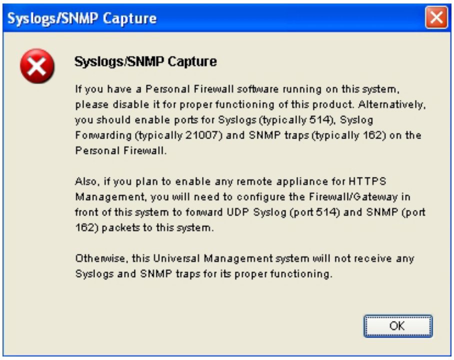
Do you want to keep blocking this program?

Name: Java(TM) Platform SE binary

Publisher: Sun Microsystems, Inc.

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

9. The installer displays a progress bar as the files are installed. Wait a few minutes for the installer to finish installing.
10. After the files are installed, whether or not the system has a Personal Firewall such as Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall if you plan to use HTTPS Management mode for managing remote appliances (instead of GMS Management Tunnel or Existing Tunnel modes). Click **OK**. Be sure to adjust the settings as recommended.



Syslogs/SNMP Capture

Syslogs/SNMP Capture

If you have a Personal Firewall software running on this system, please disable it for proper functioning of this product. Alternatively, you should enable ports for Syslogs (typically 514), Syslog Forwarding (typically 21007) and SNMP traps (typically 162) on the Personal Firewall.

Also, if you plan to enable any remote appliance for HTTPS Management, you will need to configure the Firewall/Gateway in front of this system to forward UDP Syslog (port 514) and SNMP (port 162) packets to this system.

Otherwise, this Universal Management system will not receive any Syslogs and SNMP traps for its proper functioning.

11. The Important Registration Information screen provides the URL and credentials to use to log into the SonicWALL GMS Universal Management Host system interface after restarting your system:

    The default URL for accessing the interface from the local system is:

    http://localhost:80/

    The default credentials are:

    User name – **admin**

    Password – **password**

This screen also provides information about registration. To register a SonicWALL GMS installation, use the 12-character serial number that you received when you purchased this product.

Click **Next**.

12. In the Installation Complete screen, select **Yes, restart my system** to restart your system immediately, or select **No, I will restart my system myself** to restart your system later. Click **Done**.
13. After restarting your system, you can access the SonicWALL UMH system interface to register the product and configure the GMS server settings on this system.

    Access the SonicWALL GMS UMH system interface by either clicking on the new desktop shortcut for **SonicWALL Universal Management Suite 7.0** (your default Web browser will launch **http://localhost/appliance/login**), or by pointing your browser at **http://localhost/**.
14. Log in using the username **admin** and the password **password**. You will be prompted to change your password.

Note: *You are forced to change your password the first time you login.*

To register and license SonicWALL GMS, see "Registering Associated Servers in a Distributed Deployment" on page 17.

Upgrading From an Earlier Version of SonicWALL GMS

You can use the SonicWALL UMS installer to upgrade from the GMS 6.0 to the 7.0 release. To complete registration, the system must have access to the Internet and you must have a MySonicWALL account.

When upgrading a distributed deployment, upgrade and register the primary system first. This is usually the SonicWALL GMS Console system from the original deployment. All subsequent instances of SonicWALL GMS will use the primary system's 12 character serial number when registering as components of the deployment. Each server in the distributed deployment must be upgraded and registered individually.

If the GMS Console (Web server) is set up for HTTPS management, the upgrade to GMS will preserve the HTTPS settings for the GMS Web server.

The upgrade installer checks with the SonicWALL backend to see if the SonicWALL GMS deployment has a valid support license. If it does not, then the upgrade discontinues. If the SonicWALL GMS installer detects that the SonicWALL backend site is not accessible, it prompts the user to enter an Upgrade Key. If the key is valid, it allows the upgrade to continue. If the key is invalid, the installation fails.

Note: *In a distributed environment, stop all GMS services on all GMS servers before performing an upgrade. You must upgrade all GMS servers in your deployment to the same version of SonicWALL GMS 7.0. You cannot have some servers running version 6.0 and others running 7.0.*

It is highly recommended that you backup your database, GMS installation folders, and the **<GMS installation folder>\conf\sgmsConfig.xml** file on all GMS servers prior to performing the SonicWALL GMS upgrade.

To upgrade the SonicWALL GMS software, perform the following steps:

1. Log on to your SonicWALL GMS management computer as **administrator** (Windows). Launch the SonicWALL Universal Management Suite 7.0 installer, by double-clicking the file **sw_gmsvp_win_eng_7.0.xxxx.xxxx.exe** (where “xxxx” are the exact version numbers). It may take several seconds for the InstallAnywhere self-extractor to initialize.
2. In the Introduction screen, click **Next**.
3. In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next**.
4. Wait while the installer prepares to install SonicWALL UMS on your system.
5. Click **Install** to upgrade your installation.

Note: *You must have a valid support license to upgrade your SonicWALL GMS.*

6. The Installer detects the previous installation of SonicWALL GMS. Click **Install** to proceed with the upgrade.
7. If you see a Windows Security Alert for Java, click **Unblock**.
8. The installer displays a progress bar as the files are installed. Wait a few minutes for the installer to finish installing.
9. After the files are installed, whether or not the system has a Personal Firewall such as Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall if you plan to use HTTPS Management mode for managing remote appliances (instead of GMS Management Tunnel or Existing Tunnel modes). Click **OK**. Be sure to adjust the settings as recommended.
10. The final installer screen contains the path of the installation folder, and warns you that the Universal Management Suite Web page will be launched next. Click **Done**.

Note: *When upgrading from SonicWALL GMS 6.0 to 7.0, legacy reports from GMS 6.0 will not be migrated to GMS 7.0. In GMS 7.0, you can still view legacy reports. For more information on viewing legacy reports, refer to the SonicWALL GMS 7.0 Administrator’s Guide.*

3 Registering and Licensing SonicWALL GMS

All instances of SonicWALL GMS must be registered and licensed before use. This requirement applies to both single server deployments or distributed deployments on multiple servers, to fresh or upgraded installations, and to software installations on Windows servers or to SonicWALL UMA appliances.

This section contains the following subsections:

- “Registering / Licensing SonicWALL GMS After a Fresh Install” on page 14
- “Registering Associated Servers in a Distributed Deployment” on page 17

Registering / Licensing SonicWALL GMS After a Fresh Install

SonicWALL GMS registration is performed using the SonicWALL Universal Management Host (UMH) system interface. When installing SonicWALL Universal Management Suite 7.0 on a server, or host, a Web server is installed to provide the UMH system interface. The system interface is available by default at **http://localhost/** after restarting the system.

To complete registration, the system must have access to the Internet and you must have a MySonicWALL account. The SonicWALL License Manager, available on the System > Licenses page of the UMH system interface, allows you to log in and enter your registration information on the SonicWALL registration site, mysonicwall.com.

Note: *MySonicWALL registration information is not sold or shared with any other company.*

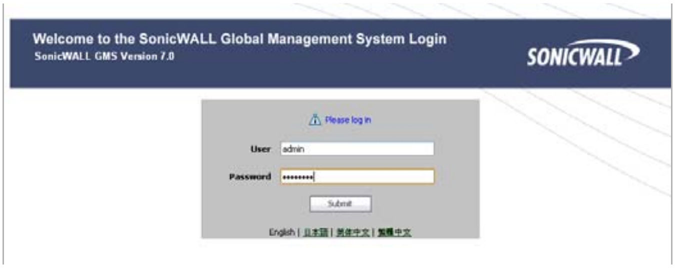
The License Manager provides a way to register the product as either SonicWALL GMS or SonicWALL Analyzer. Your choice determines the remaining installation process after registration and licensing are completed. In this guide, SonicWALL GMS registration is described.

To register and license SonicWALL GMS on this server, perform the following steps:

1. Double-click the SonicWALL Universal Management Suite 7.0 desktop icon or open a Web browser and enter **http://localhost/** to launch the UMH system interface.

Note: *If you specified a custom port (a port other than the default port 80) in* “Installing Universal Management Suite 7.0” on page 8*, modify the URL as follows:* ***http://localhost:<port>/***. *For example, if you specified port 8080, the URL would be* ***http://localhost:8080/***.

2. The login page loads by default in English, type **admin** in the **User** field, and **password** in the **Password** field and then click **Submit**. SonicWALL GMS includes language support for English, Japanese, Simplified Chinese, Traditional Chinese. Click the language of your choice at the bottom of this page.



Welcome to the SonicWALL Global Management System Login
SonicWALL GMS Version 7.0

Please log in

User admin

Password ••••••••

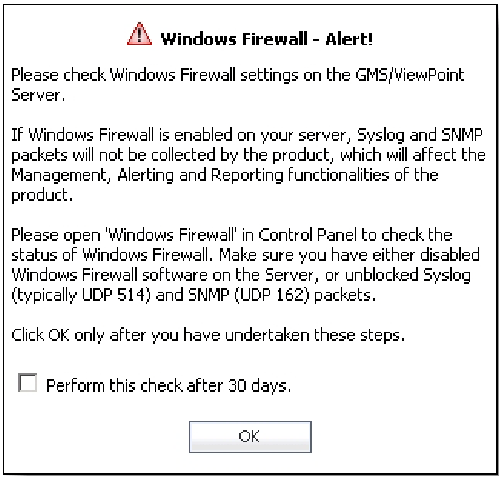
Submit

English | 日本語 | 简体中文 | 繁體中文

3. The Login page reloads to force a password change. Type a new password into both the **New Password** and **Confirm New Password** fields, and then click **Submit**.

4. If the software detects that the Windows Firewall is enabled on the system, a warning dialog box is displayed on top of the System > Status page. To receive syslog and SNMP packets, either disable the Windows Firewall or configure it to open these ports (default syslog port is UDP 514 and default SNMP port is UDP 162). When ready, click **OK**.

   Optionally, you can select the **Perform this check after 30 days** checkbox if you do not plan to disable the Windows Firewall immediately, and do not wish to see this warning every time you login. The check for Windows Firewall cannot be disabled completely, and if you leave it running you will see this alert after the 30-day delay. You can repeat the delay as many times as needed.



Windows Firewall - Alert!

Please check Windows Firewall settings on the GMS/ViewPoint Server.

If Windows Firewall is enabled on your server, Syslog and SNMP packets will not be collected by the product, which will affect the Management, Alerting and Reporting functionalities of the product.

Please open 'Windows Firewall' in Control Panel to check the status of Windows Firewall. Make sure you have either disabled Windows Firewall software on the Server, or unblocked Syslog (typically UDP 514) and SNMP (UDP 162) packets.

Click OK only after you have undertaken these steps.

□ Perform this check after 30 days.

OK

5. On the System > Status page, the **Registration Pending** notification across the top of the screen indicates that the system is not registered, the Serial Number status is **UNKNOWN**, and the License status displays **Not Licensed**. To begin registration, click the **Register** button in the top, right corner.

6. On the License Management page, type your MySonicWALL user name and password into the appropriate fields and then click **Submit**.

Note: *If you do not have a MySonicWALL account, you must create one before continuing. Click **here** in the sentence, **If you do not have a mySonicWall account, please click here to create one.***

7. On the second License Management page, type your 12-character software serial number into the **Serial Number** field and your authentication code into the **Authentication Code** field.

Note: *If this is the first SonicWALL GMS that you are registering in a multi-server deployment, the Serial Number and Authentication Code you received from your SonicWALL sales representative is entered here. As you add more instances of SonicWALL GMS on Windows Server systems to the distributed deployment, use the same serial number used for the installation of the first GMS Windows Software or SonicWALL UMA appliance. You can use the GMS Windows serial number to register associated servers if it is a full-retail GMS serial number, but not a Demo or Free Trial GMS serial number. See* "Registering Associated Servers in a Distributed Deployment" on page 17*.*

8. Type a friendly name for the system into the **Friendly Name** field. The friendly name is displayed on MySonicWALL to more easily identify the installation on this system. Click **Submit**.

Note: *If this is the first SonicWALL GMS that you have registered in a multi-server deployment, the Friendly Name for this system will also be used as the name for the distributed deployment. See* "Registering Associated Servers in a Distributed Deployment" on page 17*.*

9. The License Management page displays a completion screen. Click **Continue**.

   The License Management page displays license summary information.

After registration, the next step is to select the role for this GMS server. Continue with the procedure described in "Selecting the Role for a SonicWALL GMS Server" on page 18.

Registering Associated Servers in a Distributed Deployment

When you have a distributed SonicWALL GMS deployment involving more than one SonicWALL UMA EM5000 appliance or software instance of SonicWALL GMS, you can associate these components during the registration process. A MySonicWALL account is required. In a distributed deployment, SonicWALL GMS must be registered and licensed on each server and associated with the initially registered instance of GMS. This is accomplished by entering the serial number of the primary instance of SonicWALL GMS when registering each subsequent server in the distributed deployment.

When the primary instance of SonicWALL GMS is a SonicWALL UMA EM5000 appliance, you can download the SonicWALL UMS installer from MySonicWALL, so that you can install SonicWALL UMS on Windows systems to be used in the distributed deployment. When registering the software instances of SonicWALL GMS, use the serial number of the SonicWALL UMA appliance.

Note: *The base 10-node or 25-node management license is not automatically increased when additional servers are associated with an existing SonicWALL GMS deployment. You can purchase additional node licenses on MySonicWALL.*

To register a SonicWALL GMS instance as an associated server in an existing SonicWALL GMS deployment, perform the following steps:

1. In a browser, log into the system management interface and click the **Register** button.
2. On the License Management page, enter the same MySonicWALL user name and password that you used when registering the primary instance of SonicWALL GMS into the appropriate fields and then click **Submit**.
3. On the second License Management page, do one of the following:
   - Type the 12 character serial number of the primary SonicWALL GMS into the **Serial Number** field and type the authentication code of the primary SonicWALL GMS into the **Authentication Code** field. The primary SonicWALL GMS must already be registered.
   - If adding a SonicWALL UMA EM5000 as a secondary member of a distributed deployment, the License Manager automatically populates the **Serial Number** field. You will have the opportunity to add this unit to the existing deployment in a later step.
   - If you have an 8 character serial number because you upgraded this distributed deployment from a previous version of SonicWALL GMS, click the **Click here if you have an 8 character Serial Number** link and enter the 8 character serial number of the primary SonicWALL GMS.
4. Type a descriptive name for the system into the **Friendly Name** field. Click **Submit**.
5. In the License Management completion screen, click **Continue**.

After registration, the next step is to select the role for this GMS server. Continue with the procedure described in “Selecting the Role for a SonicWALL GMS Server” on page 18.

4 Selecting the Role for a SonicWALL GMS Server

The role that you assign to your SonicWALL GMS defines the SonicWALL Universal Management Suite services that it will provide. SonicWALL GMS uses these services to perform management, monitoring, and reporting tasks.

Your SonicWALL GMS can be deployed in any of the following roles:

- All in One
- Database Only
- Console
- Agent
- Monitor
- Syslog Collector

In the UMH system interface, clicking **Details** in the same row as a role provides a list of the services that run on a system in that role, and information about using the role.

As the number of managed appliances increases, a more distributed deployment provides better performance. To manage large numbers of SonicWALL appliances, you can use several SonicWALL GMS instances operating in different roles in a distributed deployment. These instances can run on Windows Server machines or on SonicWALL UMA appliances.

You can include the MySQL database installation with any role. The All In One or Database Only roles automatically include the MySQL database. Only one server in a SonicWALL GMS deployment should have the MySQL database included in its role.

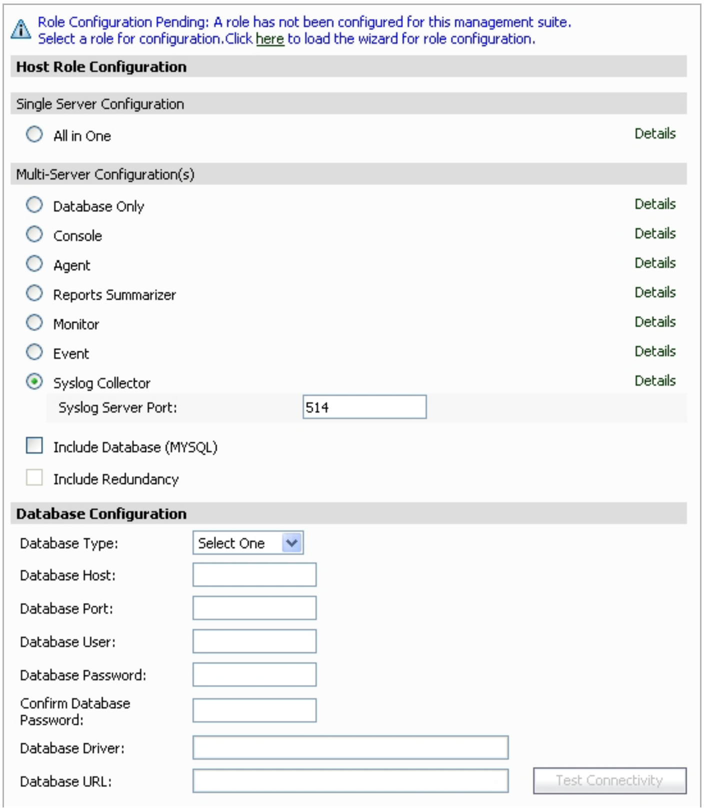
You can scale your deployment to handle more units and more reporting by adding more systems in the Agent role. Agents provide built-in redundancy capability, meaning that if an Agent goes down, other Agents can perform the configuration tasks and other tasks of the Agent that went down.

Note: *When configuring the role for the first appliance in a distributed deployment, you should either include the database or be prepared to provide the IP address of an existing database server.*

You can meet this database objective in one of the following ways:

- By selecting a role that includes the database automatically, such as **All In One** or **Database Only**
- By selecting the **Include Database (MYSQL)** checkbox if configuring the system with any other role
- By setting up a compatible database on another machine and providing that IP address when prompted

The initial **Deployment** > **Role** page is shown below:



Role Configuration Pending: A role has not been configured for this management suite.
Select a role for configuration.Click here to load the wizard for role configuration.

Host Role Configuration

Single Server Configuration

○ All in One — Details

Multi-Server Configuration(s)

○ Database Only — Details
○ Console — Details
○ Agent — Details
○ Reports Summarizer — Details
○ Monitor — Details
○ Event — Details
● Syslog Collector — Details

Syslog Server Port: 514

□ Include Database (MYSQL)
□ Include Redundancy

Database Configuration

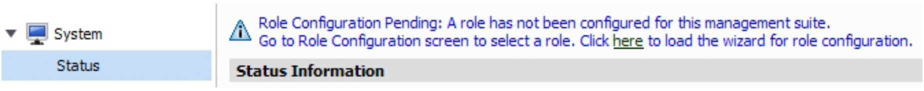
Database Type: Select One
Database Host:
Database Port:
Database User:
Database Password:
Confirm Database Password:
Database Driver:
Database URL:

Using the Role Configuration Tool

The Role Configuration Tool is a wizard that guides you through the process of defining the deployment role for SonicWALL GMS. Your system must be registered and licensed for SonicWALL GMS to run the Role Configuration Tool.

There are two ways to access the Role Configuration Tool:

- After the appliance is registered and licensed for SonicWALL GMS, the **System** > **Status** page of the appliance management interface provides a link to the wizard.



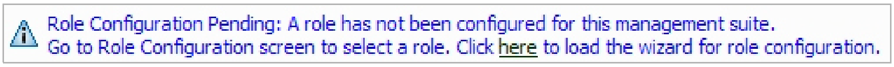
Role Configuration Pending: A role has not been configured for this management suite.
Go to Role Configuration screen to select a role. Click here to load the wizard for role configuration.

Status Information

- The **Wizards** button in the top right corner of the page provides access to the Role Configuration Tool.

To use the Role Configuration Tool, perform the following steps:

1. Log into the appliance management interface and navigate to the **System > Status** page.
2. Click the **Click here** link at the top of the page.



Role Configuration Pending: A role has not been configured for this management suite.
Go to Role Configuration screen to select a role. Click here to load the wizard for role configuration.

3. In the Introduction page of the Role Configuration Tool, click **Next**.
4. In the Setup Type page, select **Yes** if you are adding this system to an existing SonicWALL GMS deployment. Selecting Yes indicates to the wizard that there is an existing SonicWALL GMS database on another server. Select **No** if this system is part of a new SonicWALL GMS deployment or is the only system in your GMS deployment. Click **Next**.

Note: *If you selected Yes, skip step 5 and proceed to step 6.*

5. In the Deployment Type page, select **Yes** if this system will be the only SonicWALL GMS server in the deployment, or select **No** if there will be multiple GMS servers. Click **Next.**
6. In the Role Configuration page, select the desired role for this system and select the **Include Database (MYSQL)** checkbox if you want to configure a SonicWALL GMS database on this system. Click **Next**.

   The list of roles on this page will vary depending on your previous selections such as whether this system is part of an existing SonicWALL GMS deployment and if it is a single-server or part of a multi-server deployment. Neither the Database Only nor the Include Database (MYSQL) options are available if this system is part of an existing deployment.
7. In the Database Configuration page, enter the database parameters that are required for the selected role. The database fields will vary depending on your previous selections.

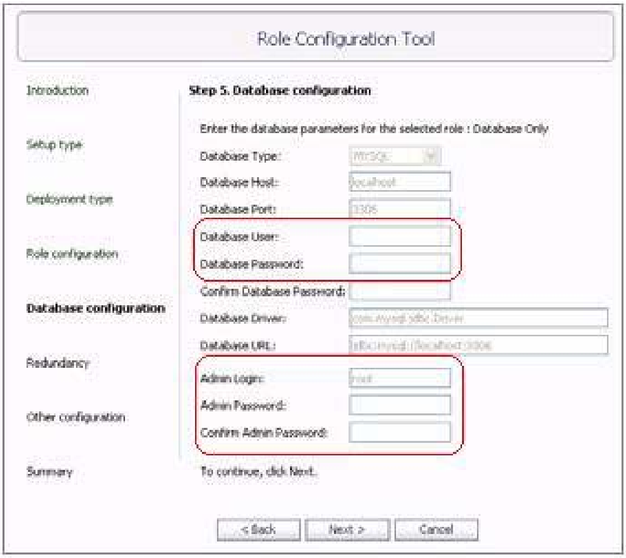
   Certain fields will be prepopulated if you made a choice of role that automatically includes the MySQL database or if you chose **Include Database (MYSQL)**.

   For a MySQL instance, additional fields are available for configuring the database administrator credentials. The **Administrator Credentials** fields are only displayed and editable in the following circumstances:

   - The **Database Type** is **MySQL**
   - The **Include Database (MYSQL)** checkbox is selected either manually or automatically for the chosen role
   - The **Database Host** field is set to **localhost** and is not editable

   When these conditions are met, the administrator password is required to create a regular access user account for the SonicWALL GMS application.

If you selected a role that does not include the MySQL database, you have the option of configuring the use of a SQL Server database in this screen.



Step 5. Database configuration

Enter the database parameters for the selected role : Database Only

Database Type: MySQL

Database Host: localhost

Database Port: 3306

Database User:

Database Password:

Confirm Database Password:

Database Driver: com.mysql.jdbc.Driver

Database URL: jdbc:mysql://localhost:3306

Admin Login: root

Admin Password:

Confirm Admin Password:

To continue, click Next.

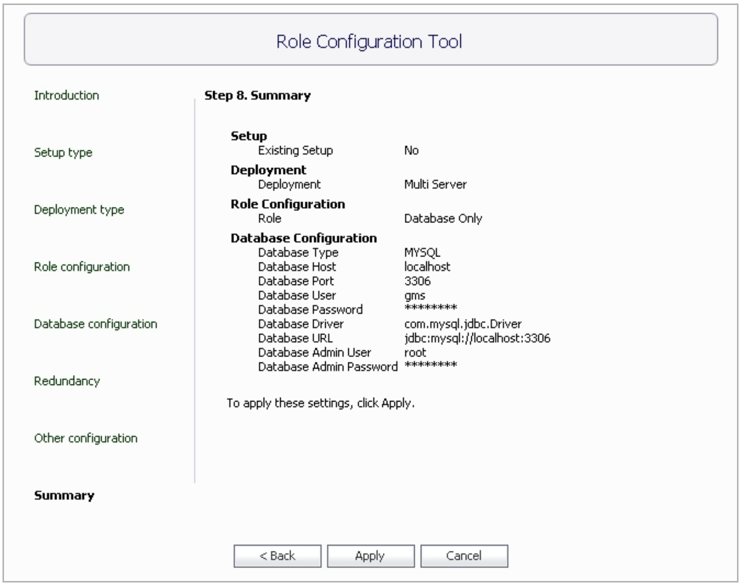
- Note the following when selecting values for these fields:
- **Database User** – Do not use any special characters, and do not use 'sa', 'root', or 'admin'.
- **Database Password** – Do not use any special characters.
- **Admin Login** – If using MySQL, the default Admin Login is 'root'. This cannot be changed.
- **Admin Password** – Do not use any special characters.

When finished entering the database parameters, click **Next**.

8. In the Other Configuration page, the fields vary depending on the selected role, as follows:
   - **Gateway Parameters** – Required for All in One, Console, and Agent roles
   - **Syslog Server Parameters -** Required for All in One, Console, Agent, and Syslog Collector roles
   - **SMTP Parameters -** Required for All in One and Console roles

   Enter the **GMS Gateway IP** address and connection password, if you are using a GMS gateway. Leave these fields empty if you are using HTTP/HTTPS to connect to the managed appliances.
9. In the **Syslog Server Port** field, type in the port used for receiving syslog messages or accept the default of 514.
10. For access to email on this system, including the ability to send email alerts, type the mail server IP address into the **SMTP Server** field and enter valid email addresses for the **Sender Address** and **Administrator Address**. Click **Next**.

11. In the Summary page, verify that all parameters are correct. Click **Back** to make changes on a previous screen, or click **Apply** to accept the settings.

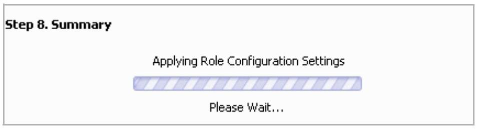


Step 8. Summary

Setup
Existing Setup No
Deployment
Deployment Multi Server
Role Configuration
Role Database Only
Database Configuration
Database Type MYSQL
Database Host localhost
Database Port 3306
Database User gms
Database Password ********
Database Driver com.mysql.jdbc.Driver
Database URL jdbc:mysql://localhost:3306
Database Admin User root
Database Admin Password ********

To apply these settings, click Apply.

12. Wait for the settings to be applied. The screen displays a progress bar until it finishes, and then displays the status. This phase can take up to 10 minutes, especially if the database was included in the deployment.



Step 8. Summary

Applying Role Configuration Settings

Please Wait...

13. Click **Close** to exit the Role Configuration Tool.

Manually Configuring the System Role

You can configure the role of the SonicWALL GMS system without using the Role Configuration Tool. All role configuration is performed in the UMH system interface, available at the URL: **http://*<IP address>*:*<port>*/appliance/**

Refer to the following sections for instructions on manually configuring the system role:

- “Configuring the All In One Role” on page 23
- “Configuring the Database Only Role” on page 24
- “Configuring the Console Role” on page 24
- “Configuring the Agent Role” on page 25
- “Configuring the Monitor Role” on page 27
- “Configuring the Syslog Collector Role” on page 27
- “Configuring Database Settings” on page 28
- “Configuring Deployment Settings” on page 29

Configuring the All In One Role

All In One deployments are ideal for managing a small number of SonicWALL appliances or for test environments. However, SonicWALL recommends that you use a multi-system, distributed deployment in production environments, with the database on a dedicated server and the other services on one or more systems. When only one other system is deployed, the Console role should be assigned to it.

The All In One role provides all eleven services utilized by SonicWALL GMS:

- Database
- Event Manager
- Monitoring Manager
- Reports Database
- Reports Scheduler
- Reports Summarizer
- Scheduler
- Syslog Collector
- Update Manager
- Web Server
- Web Service Server

To deploy your SonicWALL GMS server in the All In One role, perform the following steps:

1. Log into your UMH system interface by pointing your browser at the URL: **http://localhost/**
2. On the **Deployment > Role** page under **Host Role Configuration**, select the **All In One** radio button.
3. If this SonicWALL GMS server will connect to managed appliances through a GMS gateway, type the gateway IP address into the **GMS Gateway IP** field. To determine if a GMS gateway is required, see the *SonicWALL GMS Gateway Recommendations* section, on page 6.
4. If a GMS gateway will be used, type the password into both the **GMS Gateway Password** and **Confirm GMS Gateway Password** fields.
5. If this SonicWALL GMS server listens for syslog messages on a non-standard port, type the port number into the **Syslog Server Port** field. The default port is 514.
6. Configure the database settings as described in the *Configuring Database Settings* section, on page 28.
7. Configure the Web port settings as described in the *Configuring Web Port Settings* section, on page 30.
8. To apply your changes, click **Update**.
   To change the settings on this page back to the defaults, click **Reset**.

Configuring the Database Only Role

The Database Only role is used in a multi-server SonicWALL GMS deployment. In this role, the server is configured to run only the database service. SonicWALL recommends that one of the servers in a multi-server GMS deployment is assigned a Database Only role.

Only the SonicWALL Universal Management Suite Database service runs on a Database Only system.

SonicWALL GMS can use a MySQL database installed on a SonicWALL UMA EM5000 appliance or on a server, or a Microsoft SQL Server database installed on a server. Only the MySQL database included in the installer is supported. If upgrading from a SonicWALL GMS 5.0 installation that used the SonicWALL MySQL installer, SonicWALL GMS 7.0 will continue to support that MySQL installation.

On the Deployment > Role page in the UMH system interface, you can configure your SonicWALL GMS systems to use either a MySQL or a SQL Server database.

To deploy your SonicWALL GMS in the Database Only role, perform the steps described in the *Configuring Database Settings* section, on page 28.

Configuring the Console Role

The Console role is used in a multi-server, distributed SonicWALL GMS deployment. In this role, the SonicWALL GMS server will run all SonicWALL Universal Management Suite services except for the Database. In this scenario, the Database role is assigned to a separate appliance or server.

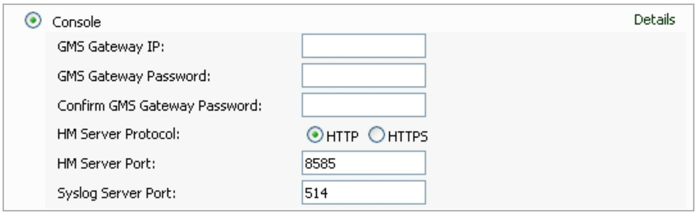
In the Console role, the SonicWALL GMS server behaves as an Agent, and also provides the following functions:

- Provides Web user interface for the SonicWALL GMS application
- Emails Scheduled Reports
- Performs Event Management tasks
- Performs various periodic checks, such as checking for new appliances that can be managed, checking for new firmware versions of managed appliances, and similar functions

Note: *In a multi-server deployment of GMS, configure port 5029 for the GMS Console Server to allow the central Web Server to communicate with the reporting databases to all GMS agents.*

To deploy your SonicWALL GMS server in the Console role, perform the following steps:

1. Log into your UMH system interface and navigate to the **Deployment > Role** page.
2. Under **Host Role Configuration**, select the **Console** radio button.



● Console

Details

GMS Gateway IP:	
GMS Gateway Password:	
Confirm GMS Gateway Password:	
HM Server Protocol:	● HTTP ○ HTTPS
HM Server Port:	8585
Syslog Server Port:	514

3. If this SonicWALL GMS server will connect to managed appliances through a GMS gateway, type the gateway IP address into the **GMS Gateway IP** field. To determine if a GMS gateway is required, see the *SonicWALL GMS Gateway Recommendations* section, on page 6.
4. If a GMS gateway will be used, type the password into both the **GMS Gateway Password** and **Confirm GMS Gateway Password** fields.
5. If this SonicWALL GMS server listens for syslog messages on a non-standard port, type the port number into the **Syslog Server Port** field. The default port is 514.
6. To use a MySQL or Microsoft SQL Server database on another system, do *not* select the **Include Database (MYSQL) c**heckbox. To include the MySQL database on this system (not recommended), select this checkbox (for this configuration, select the All In One role instead of the Console role).
7. Configure the database settings as described in the *Configuring Database Settings* section, on page 28.
8. Configure the Web port settings as described in the *Configuring Web Port Settings* section, on page 30.
9. To apply your changes, click **Update**.
   To change the settings on this page back to the defaults, click **Reset**.

Configuring the Agent Role

The Agent role can be used in a distributed deployment of SonicWALL GMS. The primary functions of this role include the following:

- Manages units by acquiring them, pushing configuration tasks to the units and tracking their up/down status
- Performs monitoring based on ICMP probes, TCP probes, and SNMP OID retrievals
- Collects and stores syslog messages
- Performs report generation

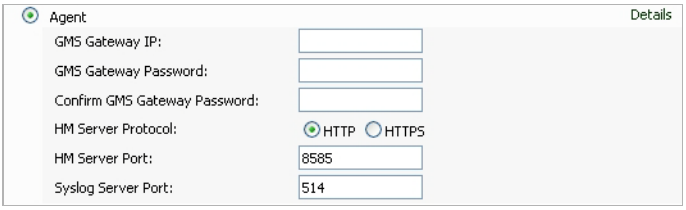
The following SonicWALL Universal Management Suite services run on an Agent system:

- Monitoring Manager
- Reports Database
- Reports Summarizer
- Scheduler

- Syslog Collector
- Web Service Server

To deploy your SonicWALL GMS server in the Agent role, perform the following steps in the UMH system interface:

1. Navigate to the **Deployment > Role** page. Under **Host Role Configuration**, select the **Agent** radio button.



● Agent

Details

GMS Gateway IP:	
GMS Gateway Password:	
Confirm GMS Gateway Password:	
HM Server Protocol:	● HTTP ○ HTTPS
HM Server Port:	8585
Syslog Server Port:	514

2. If this SonicWALL GMS server will connect to managed appliances through a GMS gateway, type the gateway IP address into the **GMS Gateway IP** field. To determine if a GMS gateway is required, see the *SonicWALL GMS Gateway Recommendations* section, on page 6.
3. If a GMS gateway will be used, type the password into both the **GMS Gateway Password** and **Confirm GMS Gateway Password** fields.
4. If this SonicWALL GMS server listens for syslog messages on a non-standard port, type the port number into the **Syslog Server Port** field. The default port is 514.
5. To include the MySQL database on this system, select the **Include Database (MYSQL)** checkbox. To use a MySQL or Microsoft SQL Server database on another system, do not select this checkbox.
6. Configure the database settings as described in the *Configuring Database Settings* section, on page 28.
7. Configure the Web port settings as described in the *Configuring Web Port Settings* section, on page 30.
8. To apply your changes, click **Update**.
   To change the settings on this page back to the defaults, click **Reset**.

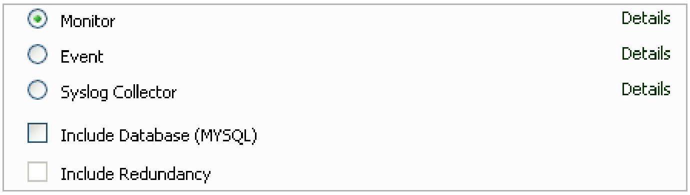
Configuring the Monitor Role

The Monitor role is used to dedicate the SonicWALL GMS server to monitoring appliances and applications in a multi-server SonicWALL GMS deployment. The monitoring is based on ICMP probes, TCP probes and SNMP OID retrievals.

Only the SonicWALL Universal Management Suite Monitoring Manager service runs on a Monitor system.

To deploy your SonicWALL GMS server in the Monitor role, perform the following steps in the UMH system interface:

1. Navigate to the **Deployment > Role** page. Under **Host Role Configuration**, select the **Monitor** radio button.



● Monitor — Details

○ Event — Details

○ Syslog Collector — Details

□ Include Database (MYSQL)

□ Include Redundancy

2. To include the MySQL database on this system, select the **Include Database (MYSQL)** checkbox. To use a MySQL or Microsoft SQL Server database on another system, do not select this checkbox.
3. Configure the database settings as described in the *Configuring Database Settings* section, on page 28.
4. Configure the Web port settings as described in the *Configuring Web Port Settings* section, on page 30.
5. To apply your changes, click **Update**.
   To change the settings on this page back to the defaults, click **Reset**.

Configuring the Syslog Collector Role

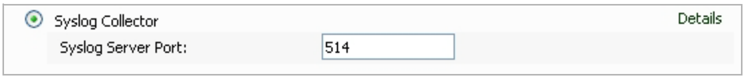
The Syslog Collector role can be assigned to a SonicWALL GMS server in a multi-server deployment of SonicWALL GMS. In this role, the SonicWALL GMS server is dedicated to collecting syslog messages on the configured port (by default, port 514). The syslog messages are stored in the SonicWALL GMS server file system.

The syslog messages are used by the Reports Summarizer service running on another SonicWALL GMS server or SonicWALL UMA EM5000 in the distributed deployment. The folder where the Syslog Collector server stores the syslog messages must be accessible by the server running the Reports Summarizer service.

Only the SonicWALL Universal Management Suite Syslog Collector service runs on a Syslog Collector system.

To deploy your SonicWALL GMS server in the Syslog Collector role, perform the following steps in the UMH system interface:

1. Navigate to the **Deployment > Role** page. Under **Host Role Configuration**, select the **Syslog Collector** radio button.



● Syslog Collector

Syslog Server Port: 514

2. If this SonicWALL GMS server listens for syslog messages on a non-standard port, type the port number into the **Syslog Server Port** field. The default port is 514.
3. To include the MySQL database on this system, select the **Include Database (MYSQL)** checkbox. To use a MySQL or Microsoft SQL Server database on another system, do not select this checkbox.
4. Configure the database settings as described in the *Configuring Database Settings* section, on page 28.
5. Configure the Web port settings as described in the *Configuring Web Port Settings* section, on page 30.
6. To apply your changes, click **Update**.
   To change the settings on this page back to the defaults, click **Reset**.

Configuring Database Settings

Database settings configuration is largely the same for any role when you choose to include the database on that server. For roles that automatically include the default MySQL database, such as All In One or Database Only, the Database Type, Database Host, and Database Port fields are not editable. This is also the case for any role when the **Include Database (MYSQL)** checkbox is selected. The Administrator Credentials fields are displayed only if the role has been defined to include the installation of the MySQL database. These are not available when a SQL Server database is selected.

This section describes the options for configuring the database settings for either the MySQL database or the Microsoft SQL Server database. SonicWALL GMS can use either a MySQL or a SQL Server database.

Note: *If this appliance will connect to a SQL Server system with a non-default instance name, then the entries will be different than described in this section. Refer to the **SonicWALL GMS Administrator's Guide** for configuration instructions.*

To configure the database settings for any role, perform the following steps in the UMH system interface:

1. Navigate to the **Deployment > Role** page and select the role for this server.
2. To run the MySQL database on this SonicWALL GMS server, select the **Include Database (MYSQL)** checkbox. To use a MySQL or Microsoft SQL Server database on another system, do not select this checkbox.
3. Under **Database Configuration**, if **Include Database (MYSQL)** was not selected in the previous step, select either **MYSQL** or **SQL Server** from the **Database Type**

drop-down list. This field is not editable if you previously selected **Include Database (MYSQL)** or if the selected role is All In One or Database Only.

4. In the **Database Host** field, type in the IP address of the database server or accept the default, **localhost**, if this SonicWALL GMS server includes the database. This field is not editable if you previously selected **Include Database (MYSQL)** or if the selected role is All In One or Database Only.
5. To use a different user name when SonicWALL GMS accesses the database, type the user name into the **Database User** field. The default user name is "sa".
6. Type the password that SonicWALL GMS will use to access the database into both the **Database Password** and **Confirm Database Password** fields.
7. Under **Administrator Credentials**, type the password for the administrator (root) account into both the **Admin Password** and **Confirm Admin Password** fields.

   Note that the **Administrator Credentials** fields are only displayed and editable in the following circumstances:

   - The **Database Type** is **MySQL**
   - The **Include Database (MYSQL)** checkbox is selected either manually or automatically for the chosen role
   - The **Database Host** field is set to **localhost** and is not editable

   When these conditions are met, the administrator password is required to create a regular access user account for the SonicWALL GMS application.
8. To apply your changes, click **Update**.
   To change the settings on this page back to the defaults, click **Reset**.

Note: *It may take 10 or 15 minutes for a database installation to complete. The database installation creates a minimal GMS database. To change database sizes, you may need to use database tools such as MySQL Server Enterprise Manager.*

Tip: *For optimal performance, you need to configure database maintenance plans. For information on configuring SonicWALL GMS maintenance plans, refer to the SonicWALL GMS Administrator's Guide.*

Configuring Deployment Settings

The following sections describes the settings available on the **Deployment** > **Settings** page of the system interface:

- "Configuring Web Port Settings" on page 30
- "Configuring SMTP Settings" on page 30
- "Configuring SSL Certificate Access" on page 31

Configuring Web Port Settings

Web port settings configuration is largely the same on any role. To change the Web port settings, perform the following steps:

1. On the **Deployment > Settings** page under **Web Port Configuration**, to use a different port for HTTP access to the SonicWALL GMS server, type the port number into the **HTTP Port** field. The default port is 80.
2. To use a different port for HTTPS access to the SonicWALL GMS server, type the port number into the **HTTPS Port** field. The default port is 443.
3. Click **Update** to apply the Web port settings.

Note: *Changing the Web port settings will cause the system to restart.*

4. After the appliance restarts, use the new port to access the appliance management interface. For example:
   - If you changed the HTTP port to 8080, use the URL: **http://**<*IP Address*>**:8080/appliance/**
   - If you changed the HTTPS port to 4430, use the URL: **http://**<*IP Address*>**:4430/appliance/**

Configuring SMTP Settings

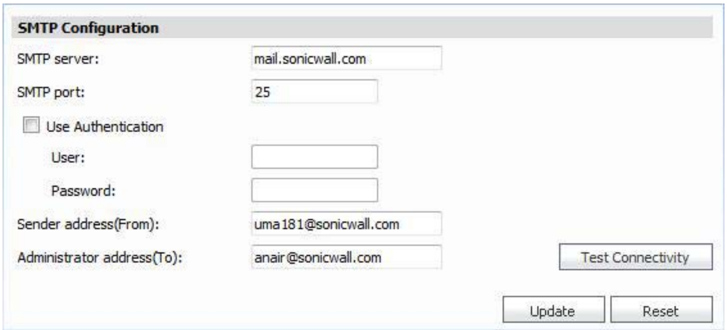
The SMTP settings are used for sending email alerts to the SonicWALL UMH system administrator.

If the Mail Server settings are not configured correctly, you will not receive important email notifications, such as:

- System alerts for your SonicWALL GMS deployment performance
- Availability of product updates, hot fixes, or patches
- Availability of firmware upgrades for managed appliances
- Alerts on your managed appliances’ status
- Scheduled Reports

To configure the SMTP settings, perform the following steps:

1. On the **Deployment > Settings** page under **SMTP Configuration**, enter the IP address of the SMTP server into the **SMTP server** field.



SMTP Configuration

SMTP server: mail.sonicwall.com

SMTP port: 25

□ Use Authentication

User:

Password:

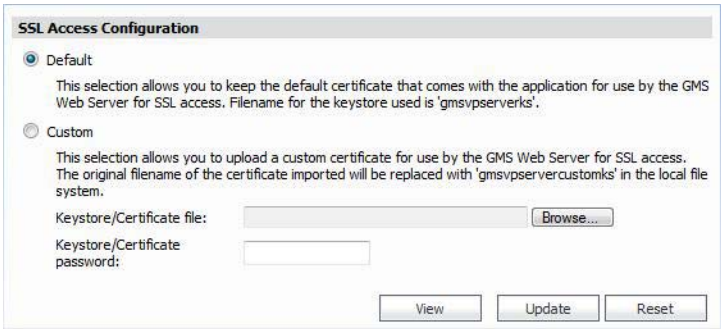
Sender address(From): uma181@sonicwall.com

Administrator address(To): anair@sonicwall.com

2. Select the **Use Authentication** checkbox, and enter your SMTP server username and password.
3. In the **Sender address** field, enter the email address that will appear as the ‘From’ address when email alerts are sent to the administrator.
4. In the **Administrator address** field, enter a valid email address for the administrator who will receive email alerts.
5. Click the **Test Connectivity** button to verify your SMTP server configuration settings.
6. Click **Update** to apply the SMTP settings.

Configuring SSL Certificate Access

Most SonicWALL GMS deployments use the default certificate accompanied with your GMS Web Server. You can also choose to use a custom certificate and a respective unique password for your SonicWALL GMS deployment as shown below.



SSL Access Configuration

● Default

This selection allows you to keep the default certificate that comes with the application for use by the GMS Web Server for SSL access. Filename for the keystore used is 'gmsvpserverks'.

○ Custom

This selection allows you to upload a custom certificate for use by the GMS Web Server for SSL access. The original filename of the certificate imported will be replaced with 'gmsvpservercustomks' in the local file system.

Keystore/Certificate file:

Keystore/Certificate password:

5 Introduction to the Management Interfaces

This section describes the two SonicWALL GMS management interfaces. An almost identical URL is used when accessing either the GMS management interface or the Universal Management Host system interface, but the URL is modified to specify either **sgms** or **appliance**.

See the following sections:

- "Overview of the Two Interfaces" on page 32
- "Switching Between Management Interfaces" on page 33
- "SonicWALL UMH System Interface Introduction" on page 33
- "SonicWALL GMS Management Interface Introduction" on page 34

Overview of the Two Interfaces

The SonicWALL GMS Universal Management Suite (UMS) installs two separate management interfaces:

- **SonicWALL Universal Management Host (UMH) System Management Interface** – Used for system management of the host server, including registration and licensing, setting the admin password, selecting the deployment role, and configuring other system settings.

  To access the UMH system management interface on the default HTTP port using a browser on the host server, use the URL:

  http://localhost/appliance/

  From another system, access the UMH system management interface with the URL:
  http://*<IP address>*:*<port>***/appliance/**

  If you are using the standard HTTP port, 80, it is not necessary to append the port number to the IP address.
- **SonicWALL GMS Management Interface** – Used to access the SonicWALL GMS application that runs on the Windows server. This interface is used to configure GMS management of SonicWALL appliances, including creating policies, viewing reports, and monitoring networks, and for configuring GMS administrative settings. The GMS management interface is only available on systems deployed in a role that runs the Web Server service, such as the All In One or Console roles.

  Access the GMS management interface with one of the following URLs:

  http://localhost/sgms/
  http://*<IP address>*:*<port>***/sgms/**

Switching Between Management Interfaces

On systems deployed in the All In One or Console role, the “superadmin” user can easily switch between the UMH system management interface and the SonicWALL GMS management interface. The SuperAdmin is the master administrator for the entire GMS installation.

When logged in to either interface, the superadmin can switch to the login page of the other interface by clicking the **Switch** button in the top right corner of the page. The **Switch** button is only visible for users with SuperAdmin privileges.

SonicWALL UMH System Interface Introduction

The SonicWALL UMH system interface is used for system management of the SonicWALL GMS instance, including registration and licensing, setting the admin password, configuring database settings, selecting the deployment role, and configuring other system settings.

When installing SonicWALL Universal Management Suite 7.0 on a host, a Web server is installed to provide the system management interface. The system interface is available by default at **http://localhost/appliance/** after restarting the system.

The login screen allows you to securely login to the SonicWALL UMH system interface using your system user ID and password.

Note: *The admin account on the system interface can have a different password than the admin account for SonicWALL GMS.*

SonicWALL GMS Management Interface Introduction

SonicWALL GMS is a Web-based application for configuring, managing, monitoring and gathering reports from thousands of SonicWALL Internet security appliances and non-SonicWALL appliances, all from a central location. This section provides an introduction to the main elements of the Web-based management interface. This section contains the following subsections:

- "Login Screen" on page 34
- "Dashboard" on page 34
- "Live Monitoring" on page 35
- "Multi-Solution Management" on page 35
- "Management Interface" on page 36

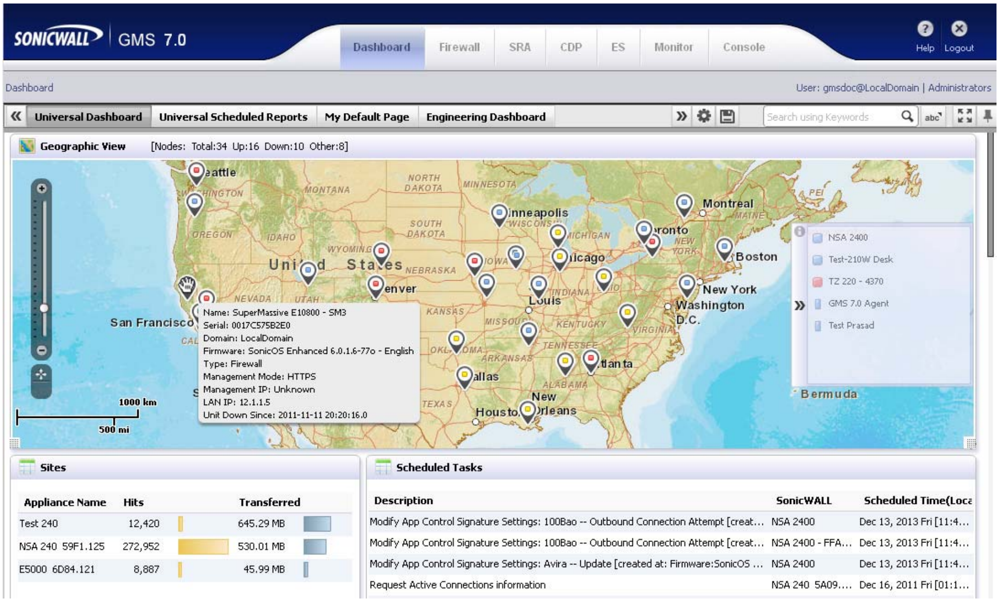
Login Screen

The login screen allows you to securely login to SonicWALL GMS using your GMS application user ID and password. The SonicWALL GMS management interface is available by default at **http://localhost/sgms/** after completing registration.

Dashboard

The Dashboard tab is a customizable dashboard of your SonicWALL GMS deployment. The Dashboard tab provides powerful network visualization reporting, monitoring, and search filtering tools consolidated into one area of the management user interface. The Dashboard tab provides administrators with an executive summary through a **Universal Dashboard** geographic map. As depicted in the screenshot below, the Geographic View provides a scalable map that displays your SonicWALL GMS-managed units and SonicWALL GMS servers using graphical icons—these icons provide system state information with a mouse over.

The Dashboard tab also provides administrators with a centralized location to create **Universal Scheduled Reports** for Firewall, SRA, CDP, and Email Security reporting solutions.



Name: SuperMassive E10800 - SM3
Serial: 0017C575B2E0
Domain: LocalDomain
Firmware: SonicOS Enhanced 6.0.1.6-77o - English
Type: Firewall
Management Mode: HTTPS
Management IP: Unknown
LAN IP: 12.1.1.5
Unit Down Since: 2011-11-11 20:20:16.0

Appliance Name	Hits	Transferred
Test 240	12,420	645.29 MB
NSA 240 59F1.125	272,952	530.01 MB
E5000 6D84.121	8,887	45.99 MB

Description	SonicWALL	Scheduled Time(Loca
Modify App Control Signature Settings: 100Bao -- Outbound Connection Attempt [creat...	NSA 2400	Dec 13, 2013 Fri [11:4...
Modify App Control Signature Settings: 100Bao -- Outbound Connection Attempt [creat...	NSA 2400 - FFA...	Dec 13, 2013 Fri [11:4...
Modify App Control Signature Settings: Avira -- Update [created at: Firmware:SonicOS ...	NSA 2400	Dec 13, 2013 Fri [11:4...
Request Active Connections information	NSA 240 5A09....	Dec 16, 2011 Fri [01:1...

For more information on configuring the Universal Dashboard and Universal Scheduled Reports, refer to the “Using the Dashboard Panel” chapter in the *SonicWALL GMS 7.0 Administrator’s Guide*.

Live Monitoring

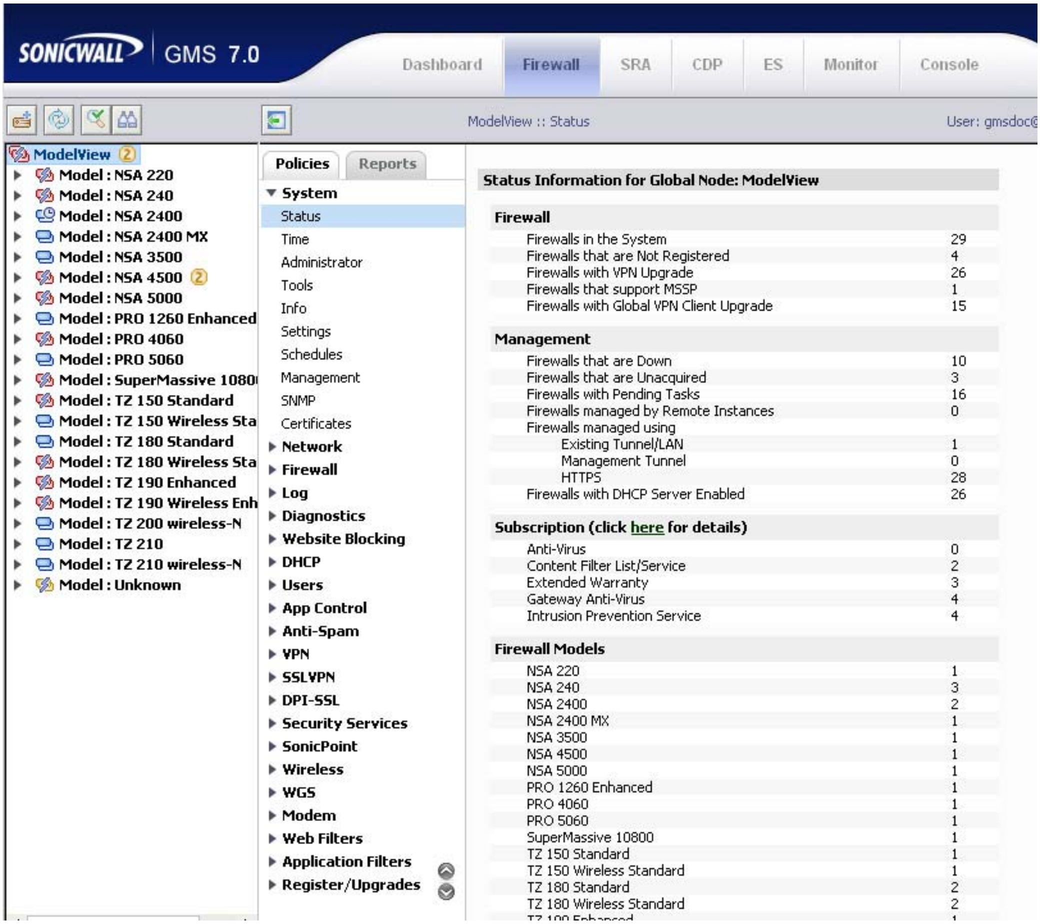
The Live Monitoring feature provides users with the ability to monitor an entire network through the correlation of syslog messages received from appliances throughout a deployment. The collected syslogs are filtered with user-defined rules to become alerts. By viewing alerts in the Live Monitoring screen, users can monitor a network, analyze traffic based on protocols, Web usage and productivity, and detect viruses and attacks in the network.

Multi-Solution Management

The Multi-Solution Management feature in SonicWALL GMS provides next generation management capability by allowing administrators to manage multiple appliance types—Firewall, CDP, SMB SRA, EX-Series SRA, and Email Security—through their respective Web user interfaces over HTTP and HTTPS. Multi-Solution Management enables GMS Core Management functionality through the GMS user interface. Functions such as creating tasks, posting policies, scheduling tasks, and more are easily completed across multiple appliances at Unit Node and Group Node levels.

Management Interface

The SonicWALL GMS management interface is the main control panel for SonicWALL GMS. The management interface allows you to add and modify appliances, perform monitoring and reporting tasks, set policies for managed appliances, and configure SonicWALL GMS settings.



Status Information for Global Node: ModelView

Firewall	
Firewalls in the System	29
Firewalls that are Not Registered	4
Firewalls with VPN Upgrade	26
Firewalls that support MSSP	1
Firewalls with Global VPN Client Upgrade	15
Management	
Firewalls that are Down	10
Firewalls that are Unacquired	3
Firewalls with Pending Tasks	16
Firewalls managed by Remote Instances	0
Firewalls managed using	
Existing Tunnel/LAN	1
Management Tunnel	0
HTTPS	28
Firewalls with DHCP Server Enabled	26
Subscription (click here for details)	
Anti-Virus	0
Content Filter List/Service	2
Extended Warranty	3
Gateway Anti-Virus	4
Intrusion Prevention Service	4
Firewall Models	
NSA 220	1
NSA 240	3
NSA 2400	2
NSA 2400 MX	1
NSA 3500	1
NSA 4500	1
NSA 5000	1
PRO 1260 Enhanced	1
PRO 4060	1
PRO 5060	1
SuperMassive 10800	1
TZ 150 Standard	1
TZ 150 Wireless Standard	1
TZ 180 Standard	2
TZ 180 Wireless Standard	2
TZ 190 Enhanced	1

The SonicWALL GMS management interface has four main sections:

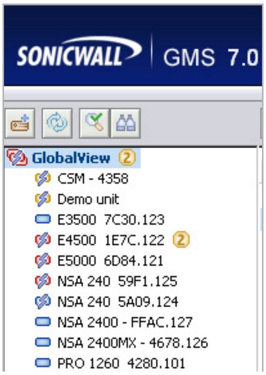
- “Navigation Tabs” on page 37
- “Left Pane” on page 37
- “Next Steps” on page 40
- “Right Pane” on page 40

Navigation Tabs

The SonicWALL GMS management interface navigation tabs are located at the top of the management interface.

The seven navigation tabs are **Dashboard, Firewall**, **SRA**, **CDP**, **ES, Monitor**, and **Console**. The **Monitor** tab provides real-time monitoring at the global, group or appliance level. The **Console** tab provides tools to customize options found in the other SonicWALL GMS tabs and to manage SonicWALL GMS settings that affect the environment globally.

Left Pane

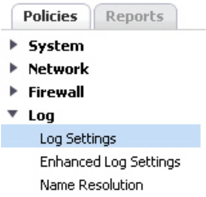


The left pane of the SonicWALL GMS management interface provides a tree control that displays the current GMS view and a list of managed appliances within the current tab. The left pane is only displayed for the four appliance tabs: **Firewall**, **SRA**, **CDP** and **ES**. The current category and view are indicated by a blue highlighting.

The left pane tree control provides the ability to switch between views and displays the current state of each appliance under management. A single box in the tree control indicates a node at appliance or unit level. Two boxes in the tree control indicates a node at a group level. A global node at the top of the tree control is indicated by a three-box icon. The color and additional images superimposed on these icons provide useful status information. For detailed information about appliance states, refer to “Right Pane” on page 38.

Note: *If there is only one appliance visible in the Left Pane, then the Left Pane will automatically collapse to present a larger screen for the rest of the UI.*

Center Pane

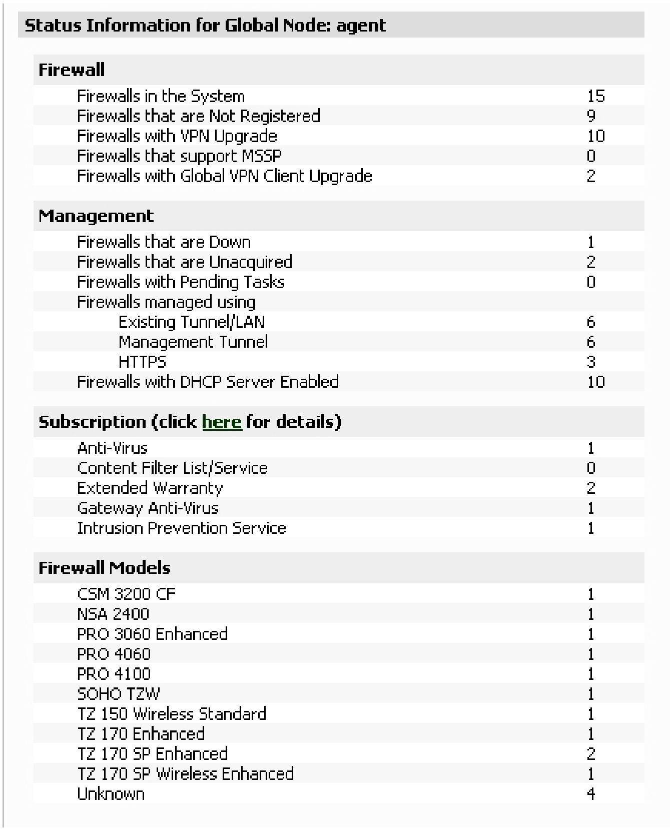


The center pane displays for the four appliance tabs: **Firewall**, **SRA**, **CDP**, and **ES**. A navigational tree control that provides access to the configuration options available based on navigational tab and left pane selections. At the top of the Center pane there are two sub-tabs, **Policies** and **Reports**. The **Policies** sub-tab provides policy configuration options for managed appliances. The **Reports** sub-tab provides reporting on the global, group, or appliance level, and is only available for **Firewall**, **SRA**, and **CDP**.

The current selection in the center pane is indicated by the highlighted item. For example, the figure to the left displays the current selection **Log** > **Log Settings**. The center pane options change based on the navigational tab and left pane selections, and selections in the center pane modify the display in the right pane. For example, the figure in the next section illustrates the contents of the right pane when the global view is selected in the left pane and **System > Status** is selected on the **Policies** tab in the center pane.

Right Pane

The right pane displays the available status or tasks based on the current selection of navigational tab, left pane and center pane options. Configurations performed in the right pane modify global, group or appliance settings. For example, the right pane image below displays the status and tasks available for the **Policies** navigation tab, left pane selection **GlobalView**, and center pane selection **System > Status**.



Status Information for Global Node: agent

Firewall	
Firewalls in the System	15
Firewalls that are Not Registered	9
Firewalls with VPN Upgrade	10
Firewalls that support MSSP	0
Firewalls with Global VPN Client Upgrade	2
Management	
Firewalls that are Down	1
Firewalls that are Unacquired	2
Firewalls with Pending Tasks	0
Firewalls managed using	
Existing Tunnel/LAN	6
Management Tunnel	6
HTTPS	3
Firewalls with DHCP Server Enabled	10
Subscription (click here for details)	
Anti-Virus	1
Content Filter List/Service	0
Extended Warranty	2
Gateway Anti-Virus	1
Intrusion Prevention Service	1
Firewall Models	
CSM 3200 CF	1
NSA 2400	1
PRO 3060 Enhanced	1
PRO 4060	1
PRO 4100	1
SOHO TZW	1
TZ 150 Wireless Standard	1
TZ 170 Enhanced	1
TZ 170 SP Enhanced	2
TZ 170 SP Wireless Enhanced	1
Unknown	4

Description of Managed Appliance States

This section describes the meaning of icons that appear next to managed appliances listed in the left pane of the SonicWALL GMS management interface.

Appliance Status	Description
🟦	One blue box indicates that the appliance is operating normally. The appliance is accessible from the SonicWALL GMS, and no tasks are pending or scheduled.
🟦🟦	Two blue boxes indicate that appliances in a group are operating normally. All appliances in the group are accessible from the SonicWALL GMS and no tasks are pending or scheduled.
🟦⚡	One blue box with a lightning flash indicates that one or more tasks are pending or running on the appliance.
🟦🟦⚡	Two blue boxes with a lightning flash indicate that tasks are currently pending or running on one or more appliances within the group.
🟦🟦🕒	Two blue boxes with a clock indicate that tasks are currently scheduled to execute at a future time on one or more appliances within the group.
🟦🕒	One blue box with a clock indicates that one or more tasks are scheduled on the appliance.
🟨	One yellow box indicates that the appliance has been added to SonicWALL GMS (provisioned) but not yet acquired.
🟨🟨	Two yellow boxes indicate that one or more appliances in the group have been added to SonicWALL GMS but not acquired.
🟨⚡	One yellow box with a lightning flash indicates that one or more tasks are pending on the provisioned appliance.
🟨🟨⚡	Two yellow boxes with a lightning flash indicates that tasks are pending on one or more provisioned appliances within the group.
🟥	One red box indicates that the appliance is not accessible from SonicWALL GMS.
🟥🟥	Two red boxes indicate that one or more appliance in the group is not accessible from SonicWALL GMS.
🟥🟥⚡	Two red boxes with a lightning flash indicate that one or more appliances in the group is not accessible from SonicWALL GMS and has one or more tasks pending.
🟥⚡	One red box with a yellow flash indicates that the appliance is not accessible from SonicWALL GMS and has one or more tasks pending.

6 Next Steps

After installation, registration, and role configuration, the next steps in setting up your SonicWALL GMS deployment are performed in the SonicWALL GMS management interface. See the *SonicWALL GMS 7.0 Administrator's Guide* for complete information about configuring SonicWALL GMS device management and reporting. This guide and other related documents are available on:
http://www.sonicwall.com/us/Support.html

Suggested next steps include the following:

- **Provisioning units** – Log into each appliance that will be managed by SonicWALL GMS, and enable GMS Management.
- **Adding units** – In the SonicWALL GMS management interface, right-click in the left navigation pane and select **Add Unit** to add a SonicWALL appliance to GMS management.
- **Scheduling reports** – Use the **Dashboard** > **Universal Scheduled Reports** panel of the SonicWALL GMS management interface to set up a reporting schedule for your managed appliances.

Copyright Notice

Specifications and descriptions subject to change without notice.

Trademarks

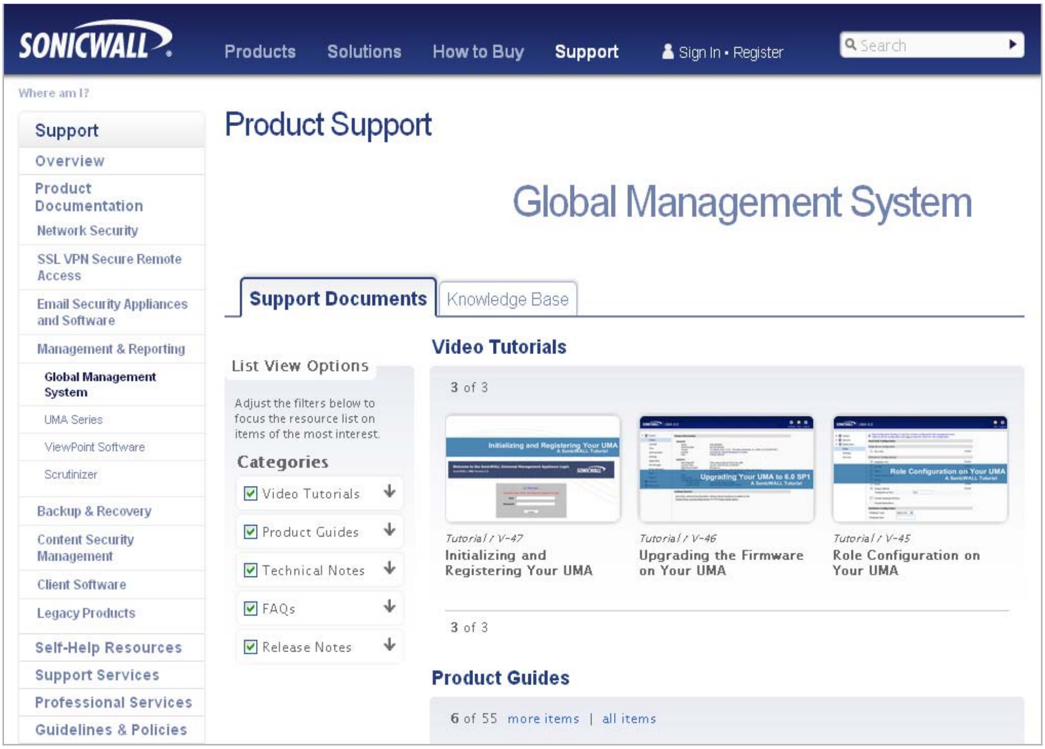
Related Technical Documentation

SonicWALL user guide reference documentation is available at the SonicWALL Technical Documentation Online Library: <http://www.sonicwall.com/us/Support.html>.

The SonicWALL GMS 7.0 documentation set includes the following user guides:

- *SonicWALL GMS 7.0 Release Notes*
- *SonicWALL GMS 7.0 Software Getting Started Guide*
- *SonicWALL GMS 7.0 Virtual Appliance Getting Started Guide*
- *SonicWALL UMA EM5000 Getting Started Guide*
- *SonicWALL GMS 7.0 Administrator's Guide*

For basic and advanced deployment examples, refer to the SonicWALL GMS user guides and deployment technotes.



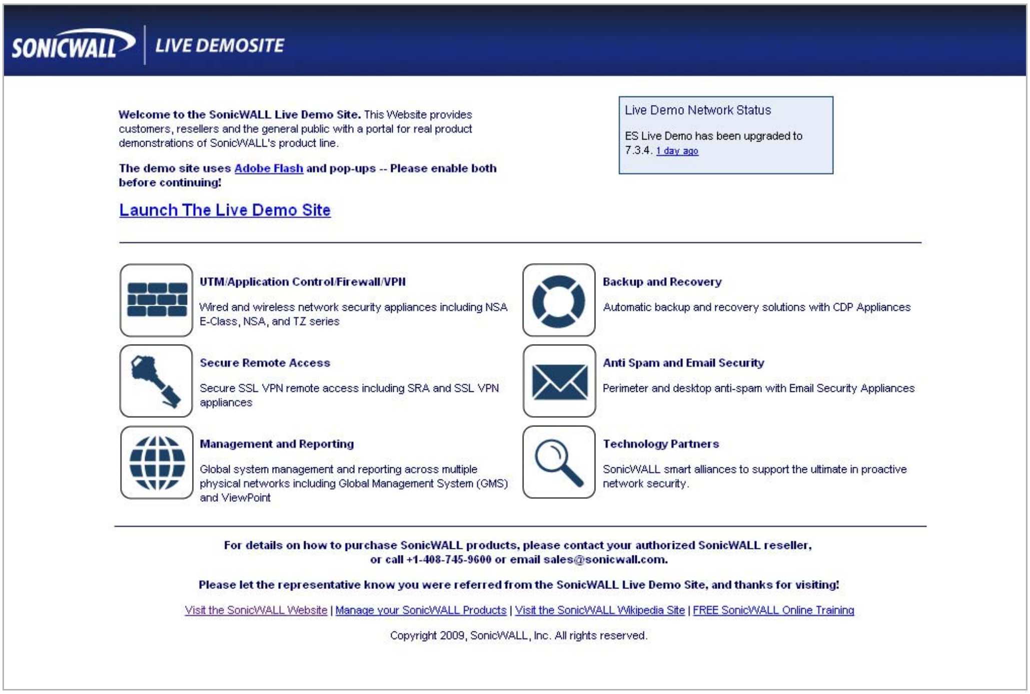
Adjust the filters below to focus the resource list on items of the most interest.

SonicWALL Live Product Demos

Get the most out of your Global Management System with the complete line of SonicWALL products. The SonicWALL Live Demo Site provides free test drives of SonicWALL security products and services through interactive live product installations:

- UTM/Firewall/VPN
- Continuous Data Protection
- SSL VPN Secure Remote Access
- Content Filtering
- Email Security
- GMS and Analyzer

For further information, visit:
<http://livedemo.sonicwall.com/>



Welcome to the SonicWALL Live Demo Site. This Website provides customers, resellers and the general public with a portal for real product demonstrations of SonicWALL's product line.

The demo site uses Adobe Flash and pop-ups -- Please enable both before continuing!

Launch The Live Demo Site

Live Demo Network Status

ES Live Demo has been upgraded to 7.3.4. 1 day ago

UTM/Application Control/Firewall/VPN
Wired and wireless network security appliances including NSA E-Class, NSA, and TZ series

Backup and Recovery
Automatic backup and recovery solutions with CDP Appliances

Secure Remote Access
Secure SSL VPN remote access including SRA and SSL VPN appliances

Anti Spam and Email Security
Perimeter and desktop anti-spam with Email Security Appliances

Management and Reporting
Global system management and reporting across multiple physical networks including Global Management System (GMS) and ViewPoint

Technology Partners
SonicWALL smart alliances to support the ultimate in proactive network security.

For details on how to purchase SonicWALL products, please contact your authorized SonicWALL reseller, or call +1-408-745-9600 or email sales@sonicwall.com.

Please let the representative know you were referred from the SonicWALL Live Demo Site, and thanks for visiting!

Visit the SonicWALL Website | Manage your SonicWALL Products | Visit the SonicWALL Wikipedia Site | FREE SonicWALL Online Training

Copyright 2009, SonicWALL, Inc. All rights reserved.

Notes

SonicWALL, Inc.

2001 Logic Drive
San Jose CA 95124-3452

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

PN: 232-000758-00   Rev B   2/12

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™